AO 106 (mod. 5/14) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

The entire property located at 8703 Berry Lane, Crandon, Wisconsin ("SUBJECT PREMISES"), including any storage or outbuildings and garages, more particularly described as a single-family mobile home located in the Town of Lincoln, Forest County. The residence is white and tan in color and has wooden additions on each end of the mobile home. Located near the front entrance door is a wooden gazebo. There is a detached garage with gray siding located on the SUBJECT PREMISES. Additionally, located on the SUBJECT PREMISES, is a small wooden shed with dark colored shingles and a "Hy Line" camper. Located near the roadside of Berry Lane is red Town of Lincoln placard with the white numerals "8703."

Case No. 19mc645

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property: See attached affidavit and attachments hereby incorporated by reference.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:
Evidence of a violation of Title 18 U.S.C. Sections 2251, 2252, and 2252A as set forth in affidavit and attachments.

The application is based on these facts: See attached affidavit.

Nathan A Cravatta
Applicant's signature

Nathan Cravatta, Special Agent
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/6/19

Judge's signature

City and State: Green Bay, Wisconsin

James R. Sickel, U.S. Magistrate Judge
Printed Name and Title

Case #19-M-645

AFFIDAVIT IN SUPPORT OF

AN APPLICATION FOR A SEARCH WARRANT

I, Nathan A. Cravatta, being duly sworn, hereby state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent with HSI since May 2005. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin.

2. My experience as an HSI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of federal law involving child exploitation, including the production, transportation, receipt, distribution and possession of child pornography. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications and the execution of searches and seizures involving computer crimes. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children which constituted violations of Title 18, United States Code, Sections 2251, 2252 and 2252A.

3. I am responsible for investigating violations of federal laws, including the offenses of advertisement, production, transportation, receipt, distribution, and possession of child pornography (as defined in Title 18, United States Code Section 2256) in interstate or foreign commerce by any means, including by computer.

4. The statements contained within this affidavit are based on my training and experience as well as the training and experience of and information communicated to me by other law enforcement personnel with whom I have personally spoken or communicated via email.

5. This affidavit is made in support of an application for warrants to search: (1) the entire premises located at 8703 Berry Lane, Crandon, Wisconsin ("SUBJECT PREMISES"), including any storage or outbuildings and garages, more particularly described as a single-family mobile home located in the Town of Lincoln, Forest County. The residence is white and tan in color and has wooden additions on each end of the mobile home. Located near the front entrance door is a wooden gazebo. There is a detached garage with gray siding located on the SUBJECT PREMISES. Additionally, located on the SUBJECT PREMISES, is a small wooden shed with dark colored shingles and a "Hy Line" camper. Located near the roadside of Berry Lane is red Town of Lincoln placard with the white numerals "8703." (2) the content of electronic storage devices located therein; and (3) any person located at the SUBJECT PREMISES in order to seize and search any electronic devices or media in his or her possession.

6. The statements in this affidavit are based in part on information provided by HSI agents in Ottawa, Canada, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

7. In my capacity as an investigator of criminal violations relating to child exploitation and child pornography, I have become familiar with the following federal statutes:

a. Receipt and Distribution of Child Pornography, 18 U.S.C. § 2252A(a)(2)(A), which makes it unlawful for someone to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Possession of Child Pornography, 18 U.S.C. § 2252A(a)(5)(B), which makes it unlawful for someone to knowingly possesses, or knowingly accesses

with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Pursuant to 18 U.S.C. § 2256(8), Child Pornography is defined as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where - (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (B) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct."

d. Pursuant to 18 U.S.C. § 2256(1), the term "minor," is defined as "any person under the age of eighteen years."

DEFINITIONS

8. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production

of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and

connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the

Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

l. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

o. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

p. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

q. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

APPLICATION A

9. "Application A" is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

10. Once downloaded and installed, the user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, "Application A" users are asked to supply a valid e-mail address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by others. Once the "Application A" user has created an account, the user is able to locate other users

via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, "Application A" users can send messages, images, and videos between two parties.

11. "Application A" also allows users to create chat rooms, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created "Application A" users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

12. "Application A" users frequently advertise their "Application A" usernames on various social networking sites in order to meet and connect with other users. In some cases, "Application A" also provides various avenues, such as dating sites and social media applications, for meeting other users. HSI undercover agents observed in some chats that many of the users stated they felt safe using "Application A" as a means of trading child pornography and for other illegal activities, due to the fact that ""Application A" is a Canadian based company, and not subject to the same United States laws." HSI undercover agents have noted messages posted in "Application A" chat rooms relating to the enforcement, deletion, or banning of users and rooms by "Application A" for the purpose of exchanging or distributing child

pornography. HSI agents noted the comments to include the continued creation of new rooms and new user accounts to circumvent "Application A's" enforcement efforts.

SUMMARY OF INVESTIGATION INVOLVING "APPLICATION A"

13. On or about April 4, 2018, "Application A" reported to the Royal Canadian Mounted Police (RCMP) that their service may have been used to distribute child pornography[1]. According to information provided to RCMP, on April 4, 2018, "Application A" user "ds18123" sent two images which depict child exploitation material on "Application A's" chat platform. I have reviewed these images and they depict the following:

a. 351320707B4A2DAF2314E60C7B791E34A0A4296D: This is a still colored image depicting a naked, prepubescent male who is lying on his back with his legs slightly spread. His penis is exposed and is the focal point of the image. His left hand is positioned near his left, upper thigh area and his head is slightly raised. Visible in the background of the image is a turquoise colored wall and a black bed post. Positioned to the right waist area of this male is another prepubescent male with shoulder length blonde hair. This male is bare chested and only his upper torso area is

[1] Canadian law requires electronic service providers to report child pornography offenses to law enforcement when they are discovered. "Application A", in partnership with law enforcement, uses hash-matching technologies to moderate images being shared between users and groups. Images sent between users are subjected to a hash calculation both before and after being optimized over "Application A's" network. When "Application A" receives notification that an image matches a hash value, a report is generated and provided to RCMP. The hash values of known child pornography being used by "Application A" have been provided by RCMP.

visible in the image. This male has the penis of the previously described male in his mouth. He also has his right hand positioned near the testicles of the other prepubescent male. "Application A" user "ds18123" sent this image on April 4, 2018 at 20:26:00 Coordinated Universal Time (UTC).

b. A9353D97296B97333851FD8C3A6E86D55D8D2798: This is a still colored image depicting an underage male who is approximately 5-8 years of age. This male is positioned to the left waist area of what appears to be an adult male. The adult male is wearing blue jeans and a gray colored shirt. The lower torso area of the adult male is visible in the lower left-hand area of the image. His jeans are pulled down to his waist exposing his penis and testicles. The left hand of the adult male is positioned near the back-head area of the underage male. The underage male has red hair and is wearing a short sleeve, turquoise colored shirt. His right hand is positioned near the penis area of the adult male. The underage male has the penis of the adult male in his mouth. Visible in the background of the image is pink blanket, black folding chair, and small portion of a white wall or trim near the head of the underage male. "Application A" user "ds18123" sent this image on April 4, 2018 at 20:24:09 UTC.

14. According to information provided by RCMP, both of the described images were posted from IP address 74.33.116.48. Open source database checks indicate this IP address resolved to Frontier Communications in Rhinelander,

Wisconsin so this investigation was subsequently forwarded to HSI Milwaukee for further investigation.

15. I reviewed the information provided by "Application A" and learned the following subscriber information for "Application A" user "ds18123":

User Name: ds18123
First Name: teen-lvr
Last Name: SC-ds18123
Email: spam26991@gmail.com (unconfirmed)

This account was registered on April 4, 2018 at 01:36:01 UTC from an Android device.

16. On May 17, 2018, I served a Department of Homeland Security administrative summons on Frontier Communications Corporation requesting subscriber information related to IP address 74.33.116.48 on the date and times "ds18123" sent the images using "Application A's" chat platform. I reviewed the information subsequently provided by Frontier Communications and saw that the IP address was assigned to "Justin Bula" at the SUBJECT PREMISES on August 18, 2016 and remained assigned to him on the date and time the images were sent using the chat platform.

17. I have queried the Wisconsin Department of Transportation (DOT) databases and learned that Justin Bula, date of birth xx/xx/1984, reported an address of the SUBJECT PREMISES. This address was updated with the Wisconsin DOT on January 6, 2012. DOT records also indicate one vehicle is registered to Justin Bula at the SUBJECT PREMISES. Registration last updated on January 22, 2018.

18. I have reviewed Forest County Assessor's Office property listing records which show that Justin Bula has owned the SUBJECT PREMISES since June 14, 2013.

19. On February 27, 2019, I spoke to Bula's supervising probation agent from the Wisconsin Department of Corrections, Division of Community Corrections. His probation agent confirmed Bula resides at the SUBJECT PREMISES and a home visit was last conducted on October 17, 2018.

20. On March 4, 2019, a representative from the U.S. Postal Service confirmed Justin Bula and Zackary Adams are receiving mail at the SUBJECT PREMISES.

21. On February 27, 2019, I reviewed the Wisconsin Sex Offender Registry. According to the Wisconsin Sex Offender Registry, the SUBJECT PREMISES is listed as being Bula's residence.

PAST CHILD EXPLOITATION CONDUCT BY JUSTIN BULA

22. According to information received from the Wisconsin Department of Justice, Division of Criminal Investigation (DCI), on August 27, 2014, DCI Special Agent (SA) Chad Racine reviewed a tip from the National Center for Missing and Exploited Children (NCMEC). According to information received, Google, Inc. identified one image uploaded in one of electronic mailing accounts that depicted content of a child engaged in sexually explicit activity. This upload was completed by an IP address which later was determined to be assigned to Northern Sandfarms Growers at the SUBJECT PREMISES.

23. On December 11, 2014, agents and officers with DCI and the Forest County Sheriff's Office executed a search warrant at the SUBJECT PREMISES. Seized and forensically previewed during the execution of the search warrant were numerous electronic devices, external storages devices, and cellular telephones. Located on media storage devices and computer hard drives were numerous images and videos depicting child exploitation material. During an interview conducted with Justin Bula, he acknowledged he had searched for, viewed, and saved files which depicted child pornography. Bula indicated he was sexually attracted to males and had seen pornographic images of males as young as infants. Bula was subsequently arrested by DCI for ten counts of Possession of Child Pornography.

24. On October 7, 2015, Justin Bula appeared in Forest County Circuit Court and was placed on probation supervision for a period of seven years. As a condition of his probation, Bula was ordered to serve 2 years in the county jail with Huber privileges. Bula is also required to comply with the Wisconsin Sex Offender Registry for the remainder of his life.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied

for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the

computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic

storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on

other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data.

Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when

the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

29. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

30. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices, smartphones, or tablets such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") and/or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are referred to as Touch ID and Face ID.

31. If a user enables a Touch ID or Face ID function on a given Apple device, smartphone, or tablet, he or she can register up to five fingerprints or the face of one person that can be used to unlock that device. The user can then use any of the registered fingerprints or the registered face to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device or hold the device up to the registered person's face. In my training and experience, users of Apple devices, smartphones, or tablets that offer Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

32. In some circumstances, a fingerprint or face cannot be used to unlock a device that has Touch ID/Face ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours (or via Face ID in 4 hours) and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, smartphone, or tablet, the opportunity to unlock the device via Touch ID or Face ID exists only for a short time. Touch ID/Face ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID/Face ID are made.

33. The passcode or password that would unlock the Apple devices, smartphones, or tablets found during the search of the premises is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the Apple devices, smartphones, or tablets found during the search of the premises to the device's Touch ID sensor or hold the phone up to the face of the devices user in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple devices, smartphones, or tablets via Touch ID with the use of the fingerprints of the user(s) or Face ID with the face of the user is necessary because the government may not otherwise be able to access the data

contained on those devices for the purpose of executing the search authorized by this warrant.

34. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints or face are among those that will unlock the device via Touch ID or Face ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the Subject Premises to press their finger(s) against the Touch ID sensor or hold up the device to their face of the locked Apple devices, smartphones, or tablets found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID or Face ID.

35. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device, smartphone, or tablet via the fingerprints on thumbs or index fingers. In the event that law enforcement is

unable to unlock the Apple devices, smartphones, or tablets found in the premises as described above within the five attempts permitted by Touch ID/Face ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

36. I request that the Court authorize law enforcement to press the fingers (including thumbs) and hold up the device to the face of individuals found at the premises to the Touch ID sensor and the camera of the Apple brand devices, smartphones, or tablets, such as an iPhone or iPad, found at the premises for the purpose of attempting to unlock the device via Touch ID and Face ID in order to search the contents as authorized by this warrant.

37. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

38. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic

storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[2]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Justin Bula uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, or on his person as set forth in Attachment A.

39. Based on the following, I believe that the user of the "ds18123" residing at the SUBJECT PREMISES likely displays characteristics common to individuals who

[2] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

distribute, possess or access with intent to view child pornography. For example, the target of this investigation:

a. "ds18123" joined and participated in "Application A's" chat platform and shared multiple images depicting child exploitation material.

b. The IP address associated with this investigation shared two images depicting child pornography.

c. Justin Bula, a subject residing at the SUBJECT PREMISES, has a prior state conviction for Possession of Child Pornography. In December 2014, the execution of a search warrant at his residence and subsequent forensic exam on electronic devices located at the residence lead to the discovery of numerous images and videos depicting child pornography.

CONCLUSION

40. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

41. I am aware that the recovery of data by a computer forensic analyst takes

significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Nathan A. Cravatta
Special Agent
U.S. Department of
Homeland Security

Sworn and subscribed before me this 6th day of March, 2019.

James R. Sickel
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 8703 Berry Lane, Crandon, Wisconsin ("SUBJECT PREMISES"), including any storage or outbuildings and garages, more particularly described as a single-family mobile home located in the Town of Lincoln, Forest County. The residence is white and tan in color and has wooden additions on each end of the mobile home. Located near the front entrance door is a wooden gazebo. There is a detached garage with gray siding located on the SUBJECT PREMISES. Additionally, located on the SUBJECT PREMISES, is a small wooden shed with dark colored shingles and a "Hy Line" camper. Located near the roadside of Berry Lane is red Town of Lincoln placard with the white numerals "8703."

The person of JUSTIN D BULA (DOB: xx/xx/1984) and ZACHARY R. ADAMS (DOB xx/xx/1983), provided that these persons are located at the SUBJECT PREMISES and/or within the Eastern District of Wisconsin at the time of the search.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 8703 Berry Lane, Crandon, Wisconsin, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Application A";

e. Records and information showing access to and/or use of "Application A"; and

f. Records and information relating or pertaining to the identity of the person or persons using or associated with "ds18123".

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular

phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) and hold up the device(s) to the face of individuals found at the premises to the Touch ID sensor of Android or Apple brand device(s) and the camera of the Apple brand devices, smartphones, or tablets, such as an iPhone or iPad, found at the premises for the purposes of attempting to unlock the device(s) via Touch ID and Face ID in order to search the contents as authorized by this warrant.